ATTACHMENT TO AMENDMENT OF May 16, 2008

(A) 依頼元発信番号(identification No.) 8091020143

発明者確認書 Inventor Declaration

私／我々は、添付に開示の発明を我々が年／月／日に着想／発明したことを宣誓する。

I/We declare that the invention disclosed in the attachment was conceived/made by me/us on

(B) [redacted] / [redacted] / [redacted] .

Year / Month / Date

(C) 発明者氏名 Inventor Name	(D) 署　名 Signature	(E) 署名日 Date	(F) 職制印 Stamp
Satoru Tanaka	田中　悟	[redacted]	[redacted]

証人確認書 Witness Declaration

私は、この書面に添付の説明書に記載の発明を確認し、理解したことを宣誓します。ここに私の理解の確認として確認日を記入し、署名及び押印致します。

I declare that I have reviewed and understood the invention disclosed in the attached paper. Here, I sign and put my stamp with the date as confirmation of my understanding.

(G) 確認者氏名 Witness Name	(G) 署　名 Signature	(I) 確認日 Date	(J) 職制印 Stamp
KAZUO IKEMOTO	池本一夫	[redacted]	[redacted]

添付資料 Attachment: 原稿・図面 (K)　[全 6 頁 (含む本頁) Total 6 Pages(including this page)]

特許明細書

[redacted]

執筆担当　FPS)第一開発部

所属氏名　田中　悟

1．発明の名称

セキュリティルーター

2．特許請求の範囲

(1) 端末のアクセスパターンによって、端末のセキュリティレベルを検出し、アクセス許可範囲を変更する方法。

(2) アクセス制限されている端末を、特定のサーバーに誘導し、ネットワーク管理者の手間を省く方法。

(3) 上記(1)～(2)を実現する装置。

3．発明の詳細な説明

（1）産業上の利用分野

本発明は、ネットワークに接続する機能を有する各種携帯情報処理装置に関するものである。

（2）従来の技術

- 特開2002-33756 アクセス制限機能付きHUB
  接続された端末のセキュリティレベルを検出する機能はなく、設定されたアクセス制限しかできない。
- 特開2001-256136(P2001-256136A) ネットワークシステム
  セキュリティを自動設定するための方法で、本発明で自動設定をより高度なものとする場合に利用できるものである。
- 特開平8-316963 端末セキュリティ管理装置
  アクセス権をユーザーや端末単位で集中管理するものであり、端末のセキュリティレベルとは関係ないものである。

（３）発明が解決しようとする課題

特定のセキュリティレベルに達していない端末がネットワークに接続された場合、それを検出することが難しかった。また、検出できても、そのセキュリティレベルを規定値にするためには、ネットワーク管理者がその都度対応する必要があった。

（４）課題を解決するための手段

図1に本発明の構成図を示す。また、図2に条件判断フローチャートを示す。

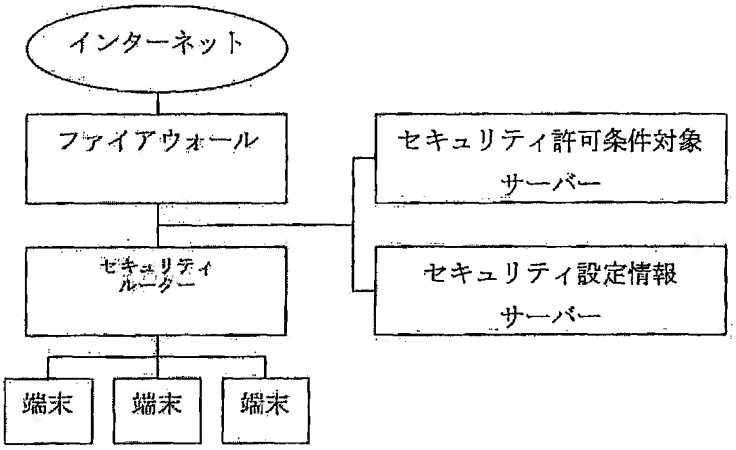

図1 構成図

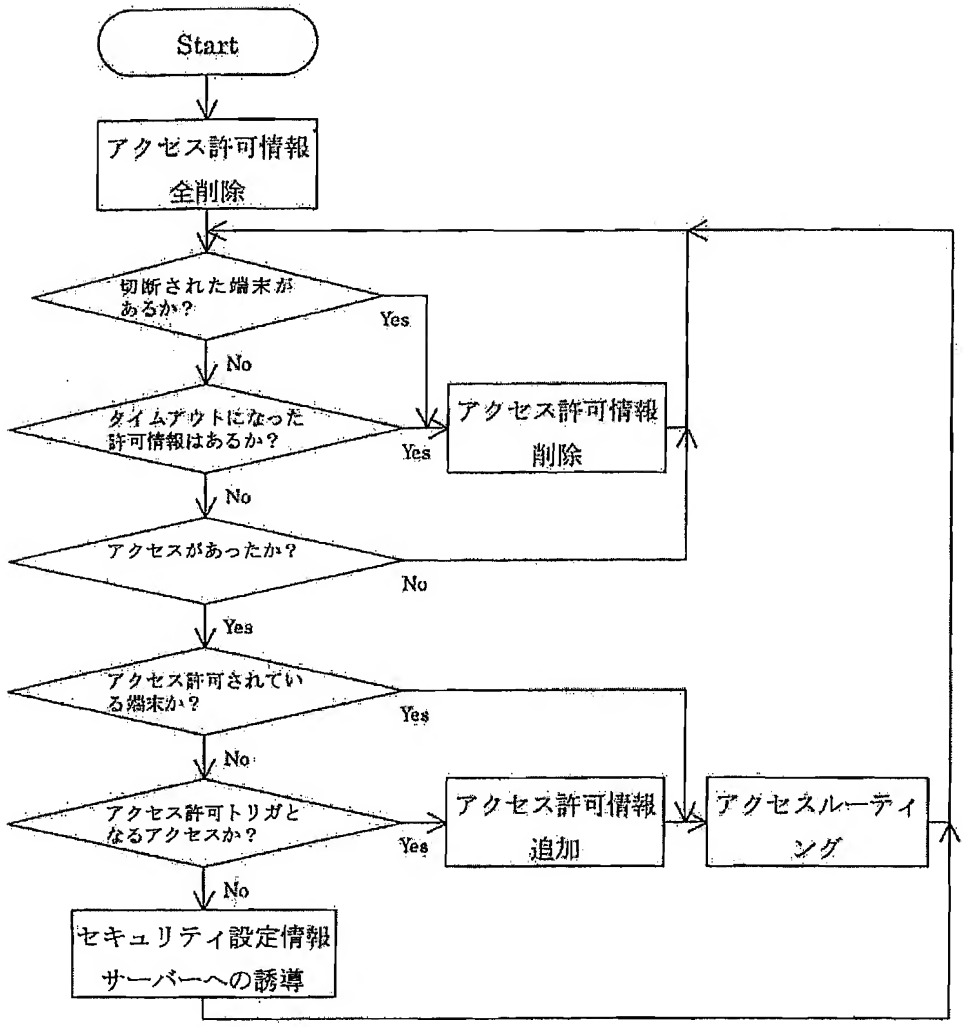

図2 条件判断フローチャート

（5）作用

端末がルーターに接続されたことを検出した場合、ある特定の動作（指定されたサーバーへのアクセス等）が検出されるまでは、セキュリティレベルが規定値に達していないと判定し、限定されたサーバーにしかアクセスできないようにする。

また、セキュリティレベルが規定値に達していない間は、一部のアクセスは自動的にセキュリティ設定案内サーバーに誘導され、ユーザーはそこの情報を元に適切な設定をすることにより、セキュリティレベルが規定値に達するように設定できる。これにより、ネットワーク管理者の手間を省くことができる。

（６）実施例

1)スタンドアロンでの実施例

ドメイン単位でセキュリティルーターを用意し、その配下に端末を接続する。

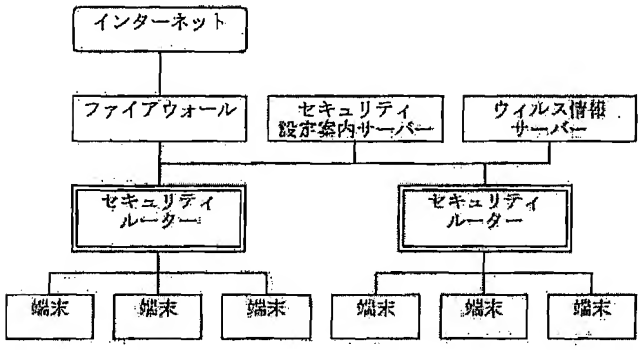

図3 ルーターでの実施イメージ

この例でのセキュリティレベルの条件は、ウィルス情報サーバーに一定間隔以内でアクセスしていることとする。また、セキュリティレベルの条件を満たしていない場合、セキュリティルーターはセキュリティ設定案内サーバーとウィルス情報サーバーにしかアクセスを許可しないとする。

特徴は、監視／制御はセキュリティルーターが全て行う点である。

2)サーバー等への組み込みでの実施例

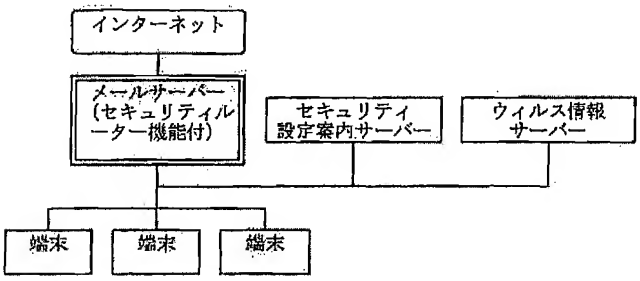

図4 サーバーでの実施イメージ

この例ではメールサーバーだが、プロキシ／NFS／ホームゲートウェイ等でも、基本的に同様になる。

この例でのセキュリティレベルの条件は、セキュリティ対象サーバー（メールサーバー）にアクセスする際は、ウィルス情報サーバーにアクセスしてから一定時間内とする。

特徴は、アクセス記録はウィルス情報サーバーが持ち、セキュリティ対象サーバーに組み込まれたルーティングプログラムがその情報を参照して、セキュリティ対象サーバーのアクセス制御を行う点である。

3)より高度な実施例

上記1)／2)において、セキュリティレベルは特定サーバーへのアクセスが基準だったが、これをセキュリティ監査プログラムからの報告とする方法である。

監査プログラムにより問題なしとなった日時から一定期間のみ、セキュリティルーターがアクセスを許可する。なお、監査記録は、端末に置く方法と、特定サーバーに集める方法がある。

（７）発明の効果

ある端末が条件を満たさない限り、セキュリティルーターはその端末のアクセスを自動的にセキュリティ設定案内サーバーに誘導し、他のドメインやサーバーにアクセスすることを禁止する。これにより、不正アクセス可能範囲を限定され、セキュリティが確保される。

一方、条件を満たしていないユーザーは、セキュリティルーターによって設定案内サーバーに誘導されるため、普通に使えるようにするための設定情報を管理者の手を煩わせることなく入手することができる。これにより、他のドメインやサーバーにアクセスできる端末は、必然的に端末のセキュリティが規定値以上に保たれることになる。

以上より、例えばウィルスに感染した端末を繋いでも、セキュリティレベルが達していないため、特定の範囲内しかアクセスできず、感染拡大を防ぐことができる。逆に、セキュリティレベルが達している端末は、アンチウィルスソフトが規定どおり動作しており、ウィルスは感染防止／駆除されるため、ウィルス感染の心配はない。

以上